The State of SELinux in Fedora

Amitosh Swain Mahapatra

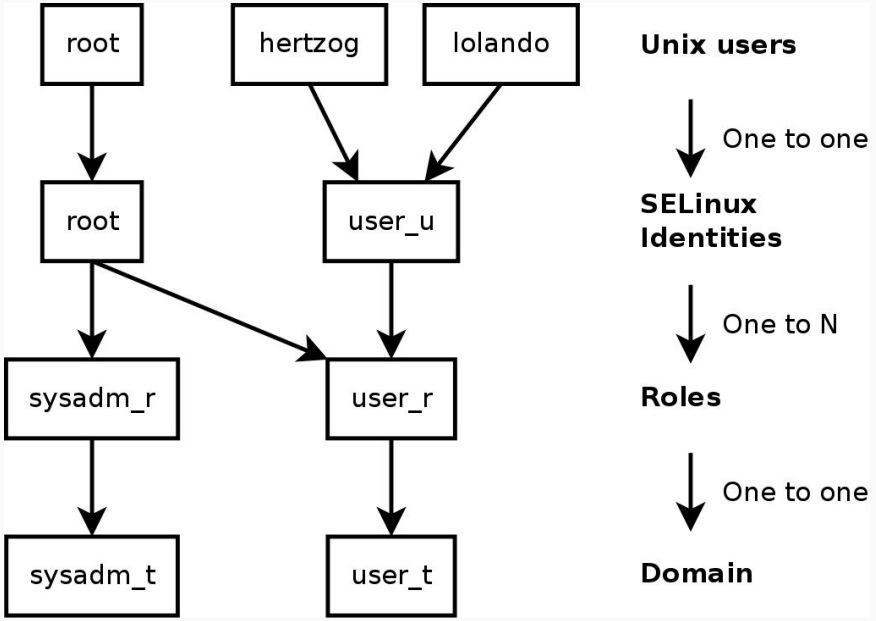
What is SELinux?

- SELinux is a mandatory access control mechanism implemented as a LSM
- Different from traditional discretionary access control. Sysadmin controls everything.
- Operates on objects and contexts stored as filesystem metadata, not on paths, opaque to things like hard links.
- It is powerful.
- But you need to configure it, it is not an IPS silver bullet.

How it Works?

- Objects have security context
- Evaluated at every syscall
- First DAC then MAC

```
system_u:object_r:passwd_exec_t:s0
User     Role     Type          Level
```




setenforce enforcing:
Do not disable
SELinux

But SELinux breaks my application!

- Use audit2allow, setroubleshoot
- File a bug at the bugzilla and let the developers know that it’s breaking.

How SELinux Progressed in Fedora

- Debuted in Fedora Core 2 (disabled by default)
- FC 3 - Enabled by default with 10 targeted policies
- FC4 - 80 Policies
- FC5 - MLS policies
- FC7 - SE Troublesoot
- FC10 - SE Policy Minimum
- FC15 - SELinux policies were starting to decompose to smaller packages
- Now - Modular policies

Where are we now?

Confining the core stuff

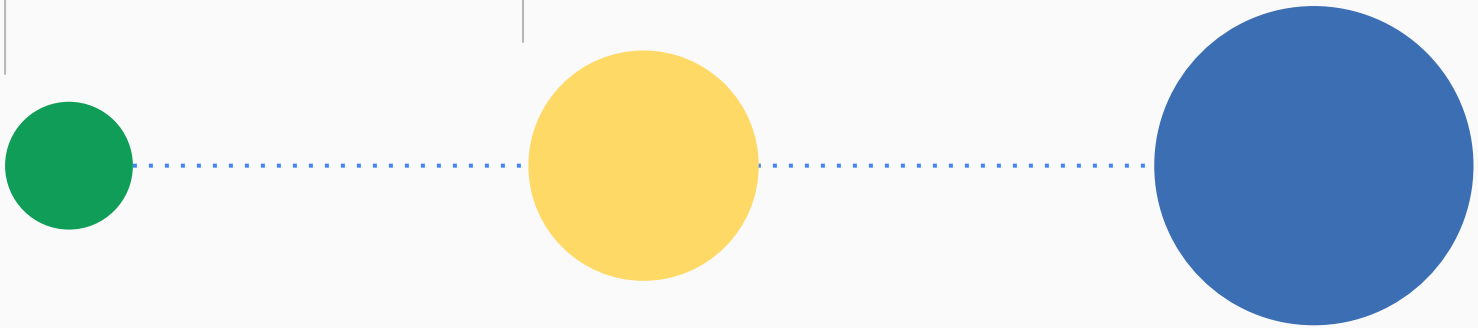
Yeah! We did it.

Cover software from repos

We are progressing

Cover everything

Complete world domination.




SELinux in
Containers

Docker and SELinux

- We have a docker-selinux policy, inspired by libvirt policies
- All files with docker_t, svirt_sandbox_file_t, `/{usr,etc}/**/*` are accessible
- Multi Category Security - For isolation between containers. (Opt-in in Fedora/RHEL/CentOS, used in CoreOS)

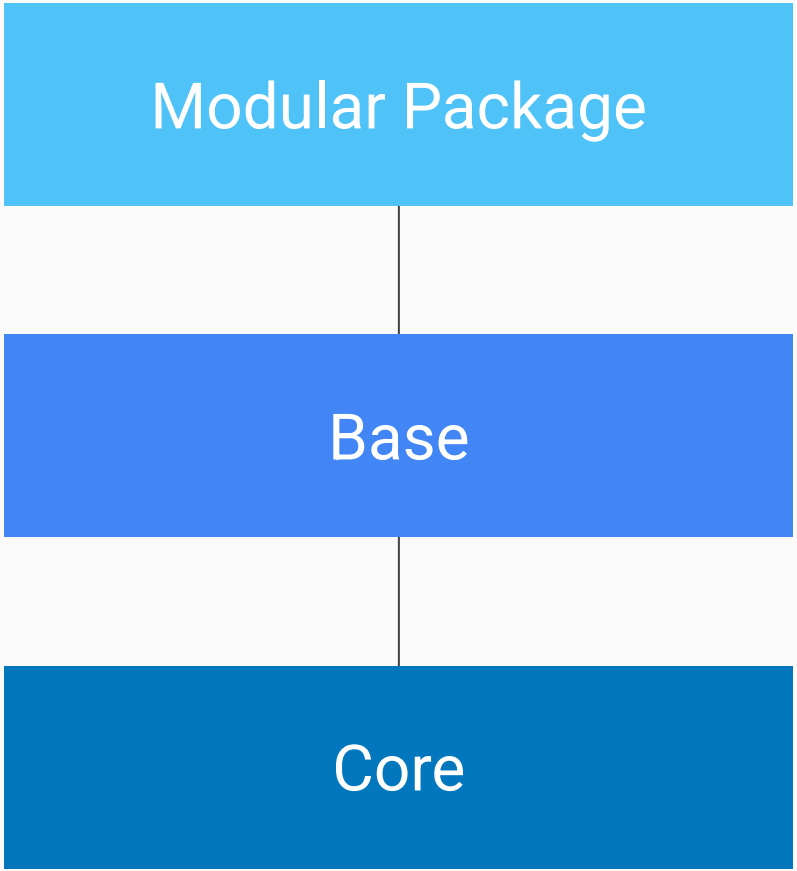
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux_atomic_host/7/html/container_security_guide/docker_selinux_security_policy

https://www.mankier.com/8/docker_selinux

Other containers

- CoreOS and rkt employs a similar security model.
- Flatpak currently doesn’t use SELinux. Running apps on different SELinux domains will provide more security against apps breaking out of the sandbox.

MODULARITY

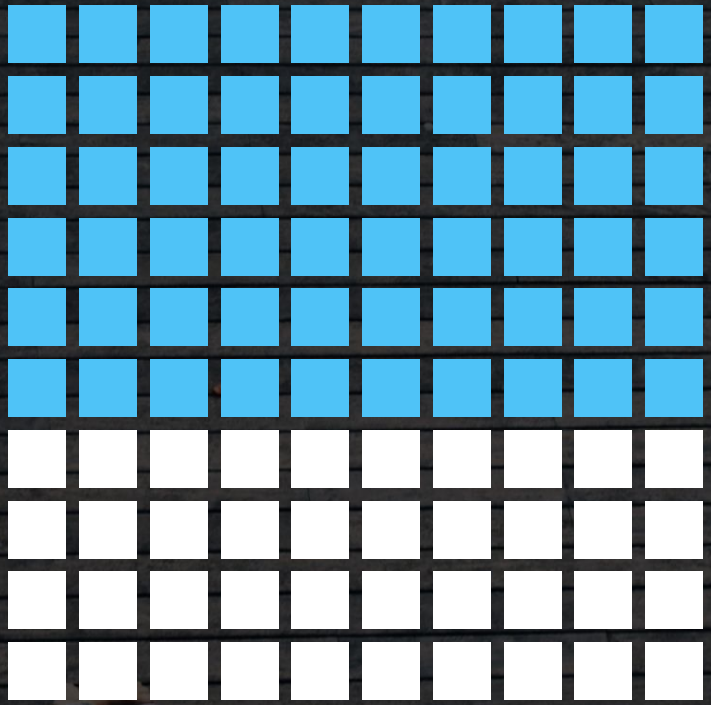


Modularity and SELinux

- Currently we have a single package (selinux-policy) that provides everything. There are few child packages and some software specific packages.
- What if version 1 of nginx uses radically different SELinux rules from version 2.
- Maintain different SELinux packages for different versions, so that it is closer to code, easier to QA and release engineering as well

Suggestions

- Gentoo Hardened
- More tools (like gensepolicy) in aiding confinement of user applications
- Addressing the fear of people wanting to use SELinux



Thank You